

criteria adopted by the Secretary at subpart C of this part.

(b) An ONC-ACB must provide the option for a Complete EHR to be certified solely to the applicable certification criteria adopted by the Secretary at subpart C of this part.

(c) *Gap certification.* An ONC-ACB may provide the option for and perform gap certification of previously certified Complete EHRs.

(d) *Inherited certified status.* An ONC-ACB must accept requests for a newer version of a previously certified Complete EHR to inherit the certified status of the previously certified Complete EHR without requiring the newer version to be recertified.

(1) Before granting certified status to a newer version of a previously certified Complete EHR, an ONC-ACB must review an attestation submitted by the developer of the Complete EHR to determine whether any change in the newer version has adversely affected the Complete EHR's capabilities for which certification criteria have been adopted.

(2) An ONC-ACB may grant certified status to a newer version of a previously certified Complete EHR if it determines that the capabilities for which certification criteria have been adopted have not been adversely affected.

(e) An ONC-ACB that has been authorized to certify Complete EHRs is also authorized to certify all EHR Modules under the permanent certification program.

§ 170.550 EHR Module certification.

(a) When certifying EHR Module(s), an ONC-ACB must certify in accordance with the applicable certification criteria adopted by the Secretary at subpart C of this part.

(b) An ONC-ACB must provide the option for an EHR Module(s) to be certified solely to the applicable certification criteria adopted by the Secretary at subpart C of this part.

(c) *Gap certification.* An ONC-ACB may provide the option for and perform gap certification of previously certified EHR Module(s).

(d) An ONC-ACB may provide an updated certification to a previously certified EHR Module(s).

(e) *Privacy and security certification.* EHR Module(s) shall be certified to all privacy and security certification criteria adopted by the Secretary, unless the EHR Module(s) is presented for certification in one of the following manners:

(1) The EHR Modules are presented for certification as a pre-coordinated, integrated bundle of EHR Modules, which would otherwise meet the definition of and constitute a Complete EHR, and one or more of the constituent EHR Modules is demonstrably responsible for providing all of the privacy and security capabilities for the entire bundle of EHR Modules; or

(2) An EHR Module is presented for certification, and the presenter can demonstrate and provide documentation to the ONC-ACB that a privacy and security certification criterion is inapplicable or that it would be technically infeasible for the EHR Module to be certified in accordance with such certification criterion.

(f) *Inherited certified status.* An ONC-ACB must accept requests for a newer version of a previously certified EHR Module(s) to inherit the certified status of the previously certified EHR Module(s) without requiring the newer version to be recertified.

(1) Before granting certified status to a newer version of a previously certified EHR Module(s), an ONC-ACB must review an attestation submitted by the developer(s) of the EHR Module(s) to determine whether any change in the newer version has adversely affected the EHR Module(s)' capabilities for which certification criteria have been adopted.

(2) An ONC-ACB may grant certified status to a newer version of a previously certified EHR Module(s) if it determines that the capabilities for which certification criteria have been adopted have not been adversely affected.

§ 170.553 Certification of health information technology other than Complete EHRs and EHR Modules.

An ONC-ACB authorized to certify health information technology other than Complete EHRs and/or EHR Modules must certify such health information technology in accordance with the